ABSTRACT

The present invention pertains to a transmission apparatus for generating an encrypted text by encrypting a plaintext, which includes a parameter storage unit for storing a random parameter (the number of terms whose coefficients indicate 1) adapted to an encryption key and an encryption apparatus and a decryption apparatus; an encryption unit for generating, from the plaintext, the encrypted text using the encryption key and the random parameter stored in the parameter storage unit, complying with an encryption algorithm based on the NTRU™ method; and a key updating unit for updating the random parameter stored in the parameter storage unit and the encryption key, as time passes.

ATTY DOCKET #: 2003_1411A **Due Date:** n/a

Confirmation No. 4208

OUR REF: 2003_1411A/MSH/01836

Applicant: Masato YAMAMICHI et al.

Serial No.: 10/680,294 **Filing Date:** October 8, 2003

Title: ENCRYPTION APPARATUS, DECRYPTION APPARATUS AND ENCRYPTION SYSTEM

Receipt of the following papers is acknowledged:

INFORMATION DISCLOSURE STATEMENT
FORM PTO-1449 w/2 references
Copy of International Search Report

Date: March 30, 2004 **Attorney:** MSH/kjf **[Check No._____]**

THE COMMISSIONER IS AUTHORIZED
TO CHARGE ANY DEFICIENCY IN THE
FEES FOR THIS PAPER TO DEPOSIT
ACCOUNT NO. 23-0975